REMARKS

Claims 1-28 and 30-45 are pending in this application. In the Office Action, the Examiner issued a final rejection of all of these claims under 35 U.S.C. 103 as being unpatentable over the prior art. In particular, Claims 1-5, 12, 14-16, 18, 23, 24, 30 and 33 were rejected as being unpatentable over U.S. Patent 6,233, 565 (Lewis, et al.) in view of U.S. Patent 5,850,442 (Muftic) and U.S. Patent 6,976,162 (Ellison, et al.). Claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35 were rejected as being unpatentable over Lewis, et al, in view of Ellison, et al.

Applicants herein ask that independent Claims 1, 6, 13, 24, 25 and 26 be amended to better define the subject matters of these claims.

Applicants respectfully submit that, for the reasons discussed below, Claims 1-28 and 30-35 patentably distinguish over the prior art and are allowable. The Examiner is, accordingly, respectfully asked to reconsider and to withdraw the above-identified rejections of Claims 1-28 and 30-35 under 35 U.S.C. 103, and to allow these claims.

Claims 1-28 and 30-35 patentably distinguish over the prior art because the prior art references do not disclose or suggest obtaining and verifying authenticity of a receipt, using two different public-private signature key pairs, and in the manner described in independent Claims 1, 6, 13, 24, 25 and 26.

As explained in detail in the present application, this invention provides procedures to issue and to verify ownership of electronic receipts while maintaining the owner of the receipt anonymous or pseudonymous. In one aspect of the invention, a user is given a pseudonym using a first pair of public/private signature keys. Using this pseudonym, the user conducts a transaction with a transaction server, which, using the public key of that first pair of public/private signature keys, issues a receipt to the user. This receipt is sent to a holder, which might be, but is not necessarily, the owner.

In another aspect of the invention, a second pair of public/private signature keys is used to verify ownership of the receipt. In particular, in accordance with this aspect of the disclosed invention, the receipt is signed using this second private signature key, and then sent to a verification server. That verification server, using the second public signature key, can verify ownership of the receipt.

The use of the two pairs of public/private signature key pairs allows the receipt to be issued and verified, while maintaining the owner of the receipt pseudonymous or anonymous. The prior art does not disclose or suggest this use of two pairs of private/public signature keys in this way.

For example, Lewis, et al, which is the primary reference relied on by the Examiner to reject the claims, describes procedures for issuing receipts over the Internet. With the system described in Lewis, et al, goods or services are purchased by a user over the Internet from a server having a receipt generation module. Special transaction software is used to manage the printing of various communications. The procedure disclosed in Lewis, et al. is relatively standard in many respects, except that it is done using the Internet. Importantly, Lewis, et al. does not disclose any specific mechanism to keep the owner anonymous or pseudonymous.

As the Examiner has recognized, there are a number of important features of the preferred embodiment of the invention that are not shown in or suggested by Lewis, et al. In order to remedy this deficiency of Lewis, et al. as a reference, the Examiner relies on a number of additional references, including Ellison, et al. and Muftic.

Ellison, et al. describes a procedure for issuing a pseudonym to protect the identity of a platform and its use. Once the platform receives this pseudonym, subsequent communications can be performed using the pseudonym to help keep the real identity of the platform anonymous.

Muftic, et al. was cited in the Office Action for its disclosure of a method and system for performing secure electronic commerce. In this method and system, procedures are used to authenticate signed messages. It is important to note that this reference is directed primarily to authentication rather than to confidentiality.

Moreover, neither Muftic, et al. nor Ellson, et al. teaches how to issue and to verify ownership of a receipt while maintaining the owner anonymous or pseudonymous.

Applicants ask that claims 1, 6, 13, 24, 15 and 26 be amended to describe more expressly the feature that two private/public signature key pairs are used to obtain and verify the authenticity of the receipt. Specifically, Claims 1 and 24 are being amended to describe the feature that a first private signature key is used to issue the receipt. These claims also describe the feature that a second private signature key is used to electronically sign a message including that receipt, and that this message is examined to determine whether it has that second private key to thereby verify its ownership while maintaining the owner anonymous or pseudonymous.

Claims 6 and 25 are directed, respectively, to a receipt generation method and receipt generating device, and Applicants herein ask that these claims be amended to describe the feature that the receipt is issued, including a reference to a designated owner and details for what the receipt has been given, in response to a message from a user using a pseudonym, where that pseudonym was issued using a first private-public key pair. As further described in these claims, the receipt can be used to verify ownership of said receipt by using a second private-public signature key pair while maintaining that owner anonymous or pseudonymous.

Claims 13 and 26 are directed to a method and apparatus, respectively, for proving ownership of a receipt. These claims, as presented herein, describe the feature that a receipt is generated in response to receiving a message created by a pseudonym that itself was issued using a first private-public signature key pair. These claims 13 and 26 describe the additional features that this receipt includes information for what the receipt has been issued and a reference to the designated owner of the receipt and thereby to enable the owner to verify ownership of said receipt by using a second private-public signature key pair while maintaining that owner anonymous or pseudonymous.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest the above-discussed use of two pairs of public/private signature key pairs.

This feature is of utility because, as discussed in the present application, it enables e-commerce to be transacted in a way that enables a person to verify ownership of a receipt while, at the same time, preserving that person's anonymity or psuedonymity.

Because of the above-discussed differences between Claims 1, 6, 13, 24, 25 and 26, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-5, 23 and 30 are dependent from Claim 1 and are allowable therewith; and Claims 7-12, 27 and 31 are dependent from, and are allowable with Claim 6. Similarly, Claims 14-22, 28 and 32 are dependent from, and are allowable with, Claim 13. Claims 33, 34 and 35 are dependent from, and are allowable with, Claims 24, 25 and 26 respectively.

The amendments requested herein only emphasize or describe in more detail features already set forth in the claims. In particular, the Claims 1, 6, 13, 24, 25 and 26 currently describe the use of private/public signature key pairs to issue a receipt and to verify its ownership, and Applicants ask that these claims be amended herein to indicate expressly that two, different key pairs are used to do this. It is thus believed that entry of this Amendment is within the discretion of the Examiner, and such entry is respectfully requested.

In view of the above discussion, the Examiner is requested to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-28 and 30-35 under 35 U.S.C. 103, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S Sensny
John S. Sensny
Registration No. 28,757
Attorney for Applicant

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy